REMARKS/ARGUMENTS

Claims 1-33 and 39-42 have been cancelled without prejudice.

<u>Claim 34</u>

Claim 34 was rejected as being anticipated by US Patent Pub 2003/0179885 to Gentry. Claim 34 has been amended to more clearly differentiate it from Gentry.

The main changes made to claim 34 are:

1.   The key generated by the method is now specified as being:

"an identifier-based asymmetric cryptographic key"

All the described embodiments generate such keys as can be readily appreciated by reference to Figure 3 and the section headed "Review" on page 16 of the application as filed.

2.   Associated with the user are:

"multiple independent identities ..., each identity being intended for use by a respective trusted authority"

Again, all the described embodiments exhibit this feature and the paragraph spanning pages 9 and 10 of the application as filed describes this feature.

3.   The secrets of the trusted authorities are specified as:

"the secrets of the trusted authorities being unrelated to each other"

That the secrets of the trusted authorities are unrelated is clear from the description - see, for example, page 9 line 16 which discloses that the trusted authorities "have their own respective random secrets", it being understood that the randomness of the secrets ensures that they are unrelated. This quoted

feature was introduce to further distinguish claim 34 from the Boneh and
Franklin paper.

The corresponding claim in the corresponding EP claim ends with the
phrase:

**"data from the multiple data sets being combined either before or after
processing by the bilinear mapping function"**

Since this sort of limitation often attracts an objection in the US, a
respective dependent claim to each possibility has been added as new claims 50
and 51. Support is easy to spot from the column headed 'General Form' in
Figure 3, for examples of either possibility.

The second of the above new features of claim 34 provides the clearest
point of difference from the Gentry reference (US 2003/0179885). In Gentry, as is
described in paragraph 0085 thereof, the recipient z is associated with the ID-
tuple:

$$(ID_{z1},....., ID_{z(n+1)})$$

This ID-tuple is made up of identity information $ID_{z(n+1)}$ associated with
the recipient z and identity information ID_{zi} associated with each of the
recipient's n ancestral lower-level PKGs in the hierarchy. In other words, each
PKG and the recipient has an identity label that is not necessarily unique in
itself but when collected in order from the root to the recipient (or, indeed, in
reverse from the recipient to the root) they make up a unique identity for the
recipient z. This is succinctly put at the top of page 551 of the Gentry paper:

> **"ID-Tuple**: A user has a position in the hierarchy, defined by its
> tuple of IDs: $(ID_1,....., ID_t)$. The user's ancestors in the
> hierarchy tree are the root PKG and the users/lower-level PKGs
> whose ID-tuples are $\{(ID_1,....., ID_i) : 1 \le i \le t\}$."

(The IDs referred to in the first line of this definition are clearly not all IDs of the user since the second sentence makes it clear that an ancestor user / lower-level PKG has an ID-tuple made up of a subset of these IDs).

Of course, ID-tuples like this are very common, two examples being domain names and street addresses (though both are usually written in reverse order).

The important point is that the recipient has only one piece of identity information associated with it ($ID_{z(n+1)}$) and only one unique identity – the ID-tuple. The identity information ID_{zi} associated with each ancestor PKG of the recipient is not specific to the recipient – any party directly or indirectly dependent from a given PKG will have the identity information of that PKG in the ID-tuple of that party. Thus Gentry does not disclose or suggest the user having:

```
"multiple independent identities …, each
identity being intended for use by a respective
trusted authority"
```

as is recited in amended claim 34.

At the top of page 6 of the Action, the examiner asserts that Gentry discloses the use of different user identities by referring to the elements U_0 to U_{n+1}. However, $U_i = rP_{zi}$ and the elements P_{zi} for $1 \le i \le n$ are public elements of the recipients ancestral PKG (see [0086]) and not of the recipient; only U_{n+1} (= $rPz(n+1)$) uses the identity information of the recipient – in particular:

$P_{z(n+1)} = H_1(ID_{z1}, \ldots., ID_{z(n+1)})$

where :

$ID_{z(n+1)}$ is the identity information of the recipient, and

$(ID_{z1}, ..., ID_{z(n+1)})$ is the ID-tuple of the recipient (the only true identifier of the recipient).

Claim 34 is also being amended to recite "using computer equipment to apply ..." to make it clear that the claim is directed to statutory subject matter.

Claim 43

Claim 43 has amended in a similar manner to the amendments made to claim 34 therefor it should be in condition for allowance.

New dependent claims 65-76 have been added which depend from claim 43 and which are patterned after the claims dependent upon claim 34.

Claim 52

Claim 52 is a new apparatus claims and its general similarity with claim 34 should be apparent and it is believed that it too distinguishes itself from the prior art.

New dependent claims 53-64 have also been added which depend from claim 52 and which are patterned after the claims dependent upon claim 34.

Figure 3

A replacement figure 3 is enclosed which corrects, as described above, minor editorial errors noted in the original version thereof.

Specification Amendment

A error was noted in the first equation of paragraph 0067 where are extra "P" occurred in the original. This amendment brings the equation into line with the disclosure at paragraph 0066.

IDS

An IDS is enclosed herewith. Enclosed therewith is an official action dated March 18, 2204, in which the European Examiner cited Boneh (which was previously cited in an IDS filed in this application.) Differentiating arguments can be found in the EP response dated June 28, 2004, a copy of which also accompanies the IDS.

The Shamir secret sharing paper listed in the IDS is cited the response dated June 28, 2004 filed in the corresponding EP application.

Two further official actions issued in respect of the corresponding EP application, but no additional prior art was cited against the claims, but clarity issues were raised. The Examiner is invited to review the prosecution history of the corresponding EP application at http://www.epoline.org/portal/public/ registerplus by providing the application number of the EP application (03254262).

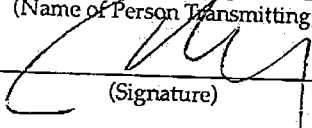Withdrawal of the rejections and allowance of the claims are respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2125. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the

number of months necessary to make this response timely filed and the petition
fee due in connection therewith may be charged to deposit account no. 08-2125.

I hereby certify that this correspondence is being
deposited with the United States Post Office with
sufficient postage as first class mail in an envelope
addressed to: Commissioner for Patents, P.O. Box 1450,
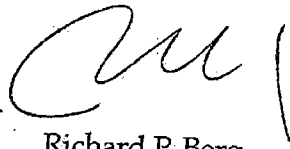Alexandria, VA 22313-1450 on

_____August 15, 2007_____
(Date of Transmission)

_____Richard Berg_____
(Name of Person Transmitting)

_____
(Signature)

_____August 15, 2007_____
(Date)

Respectfully submitted,

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile